02248
RPS

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　３月２６日

出願番号
Application Number: 特願２００３－０８５３５９

[ST. 10/C]: ［ＪＰ２００３－０８５３５９］

出願人
Applicant(s): インターナショナル・ビジネス・マシーンズ・コーポレーション

２００３年　９月１８日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０７６８６６

【書類名】　特許願

【整理番号】　JP9020248

【提出日】　平成15年 3月26日

【あて先】　特許庁長官　殿

【国際特許分類】　G06F 12/14

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内

【氏名】　麻生　純一

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内

【氏名】　與茂　孝嗣

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内

【氏名】　羽鳥　正彦

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内

【氏名】　田所　瑞穂

【特許出願人】

【識別番号】　390009531

【氏名又は名称】　インターナショナル・ビジネス・マシーンズ・コーポレーション

【代理人】

【識別番号】　100086243

【弁理士】

【氏名又は名称】　坂口　博

【代理人】
　【識別番号】　100091568
　【弁理士】
　【氏名又は名称】　市位　嘉宏
【代理人】
　【識別番号】　100108501
　【弁理士】
　【氏名又は名称】　上野　剛史
【復代理人】
　【識別番号】　100104880
　【弁理士】
　【氏名又は名称】　古部　次郎
【選任した復代理人】
　【識別番号】　100118201
　【弁理士】
　【氏名又は名称】　千田　武
【手数料の表示】
　【予納台帳番号】　081504
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9706050
　【包括委任状番号】　9704733
　【包括委任状番号】　0207860
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報処理装置、その暗号処理システム及び外部記憶装置の制御方法

【特許請求の範囲】

【請求項１】　コンピュータ本体と、

前記コンピュータ本体に設けられたコネクタを介して着脱自在に接続された外部記憶装置とを備え、

前記コンピュータ本体は、

前記外部記憶装置に対するイジェクション要求を受け付ける受け付け手段と、

前記受け付け手段にて前記イジェクション要求が受け付けられたことを条件に、前記外部記憶装置に格納されている所定のデータファイルを暗号化する暗号化手段と

を備えることを特徴とする情報処理装置。

【請求項２】　前記所定のデータファイルに対する前記暗号化手段による暗号化の完了した前記外部記憶装置へのアクセスを停止するデバイス停止手段をさらに備えることを特徴とする請求項１に記載の情報処理装置。

【請求項３】　前記暗号化手段による暗号化に用いられるパスフレーズの入力を受け付けて管理するパスフレーズ管理手段をさらに備えることを特徴とする請求項１に記載の情報処理装置。

【請求項４】　前記暗号化手段は、前記所定のデータファイルの暗号化に用いる暗号化エンジンを複数備え、当該暗号化エンジンを動的に変更して用いることを特徴とする請求項１に記載の情報処理装置。

【請求項５】　前記コネクタは、ＰＣＭＣＩＡコネクタであることを特徴とする請求項１に記載の情報処理装置。

【請求項６】　前記コネクタは、ＵＳＢコネクタであることを特徴とする請求項１に記載の情報処理装置。

【請求項７】　コンピュータ本体と、

前記コンピュータ本体に設けられたコネクタを介して着脱自在に接続された外部記憶装置とを備え、

前記コンピュータ本体は、

前記コネクタに前記外部記憶装置を接続したことによって発行される装着イベントを検出するイベント検出手段と、

前記イベント検出手段により装着が検出された前記外部記憶装置に暗号化されたデータファイルが格納されているか否かを調べる暗号化ファイル検出手段と、

前記暗号化ファイル検出手段にて検出された、暗号化されたデータファイルを、予め設定されたパスフレーズを用いて復号する復号化手段と

を備えることを特徴とする情報処理装置。

【請求項８】　前記復号化手段は、予め設定されたパスフレーズでは前記暗号化されたデータファイルを復号できない場合に、パスフレーズの入力を要求することを特徴とする請求項７に記載の情報処理装置。

【請求項９】　前記コネクタは、ＰＣＭＣＩＡコネクタであることを特徴とする請求項７に記載の情報処理装置。

【請求項１０】　前記コネクタは、ＵＳＢコネクタであることを特徴とする請求項７に記載の情報処理装置。

【請求項１１】　コンピュータに接続された外部記憶装置に格納されているデータファイルに対して暗号処理を施す暗号処理システムにおいて、

イジェクション時にデバイスへのアクセス停止処理を含むソフトウェア制御を行う仕様でコンピュータに接続された前記外部記憶装置に対するイジェクション要求を受け付ける受け付け手段と、

前記受け付け手段にて前記イジェクション要求が受け付けられたことを条件に、前記外部記憶装置に格納されている所定のデータファイルを暗号化する暗号化手段と

を備えることを特徴とする暗号処理システム。

【請求項１２】　前記コンピュータに前記外部記憶装置が接続されたことを検知して、当該外部記憶装置に格納されている暗号化されたデータファイルを復号化する復号化手段をさらに備えたことを特徴とする請求項１１に記載の暗号処理システム。

【請求項１３】　前記暗号化手段による暗号化および前記復号化手段による

復号化に用いられるパスフレーズを管理するパスフレーズ管理手段をさらに備えることを特徴とする請求項１２に記載の暗号処理システム。

【請求項１４】　コンピュータに接続された外部記憶装置の制御方法であって、

ユーザによる操作を受け付けて、イジェクション時にデバイスへのアクセス停止処理を含むソフトウェア制御を行う仕様でコンピュータに接続された前記外部記憶装置に対するイジェクション要求を発行するステップと、

前記イジェクション要求が発行されたことを条件に、前記外部記憶装置に格納されている所定のデータファイルを読み出して暗号化し、当該外部記憶装置に格納するステップと

を含むことを特徴とする外部記憶装置の制御方法。

【請求項１５】　コンピュータに接続された外部記憶装置の制御方法であって、

前記コンピュータに前記外部記憶装置が接続されたことを検知して、当該外部記憶装置に暗号化されたデータファイルが格納されているか否かを調べるステップと、

前記外部記憶装置に暗号化されたデータファイルが格納されている場合に、当該暗号化されたデータファイルを読み出し、予め設定され所定の記憶手段にて保持されているパスフレーズを用いて当該暗号化されたデータファイルを復号し、当該外部記憶装置に格納するステップと

を含むことを特徴とする外部記憶装置の制御方法。

【請求項１６】　コンピュータを制御して、当該コンピュータに接続された外部記憶装置に格納されているデータファイルに対して暗号処理を施すプログラムであって、

イジェクション時にデバイスへのアクセス停止処理を含むソフトウェア制御を行う仕様でコンピュータに接続された前記外部記憶装置に対するイジェクション要求を受け付ける受け付け手段と、

前記受け付け手段にて前記イジェクション要求が受け付けられたことを条件に、前記外部記憶装置に格納されている所定のデータファイルを暗号化する暗号化

手段として、

前記コンピュータを機能させることを特徴とするプログラム。

【請求項１７】　前記コンピュータに前記外部記憶装置が接続されたことを検知して、当該外部記憶装置に格納されている暗号化されたデータファイルを復号化する復号化手段として、前記コンピュータをさらに機能させることを特徴とする請求項１６に記載のプログラム。

【請求項１８】　前記暗号化手段による暗号化および前記復号化手段による復号化に用いられるパスフレーズを管理するパスフレーズ管理手段として、前記コンピュータをさらに機能させることを特徴とする請求項１７に記載のプログラム。

【請求項１９】　コンピュータを制御して、当該コンピュータに接続された外部記憶装置に格納されているデータファイルに対して暗号処理を施すプログラムであって、

前記コンピュータに前記外部記憶装置が接続されたことを検知して、当該外部記憶装置に暗号化されたデータファイルが格納されているか否かを調べる処理と、

前記外部記憶装置に暗号化されたデータファイルが格納されている場合に、当該暗号化されたデータファイルを読み出し、予め設定され所定の記憶手段にて保持されているパスフレーズを用いて当該暗号化されたデータファイルを復号し、当該外部記憶装置に格納する処理と

を前記コンピュータに実行させることを特徴とするプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報処理装置におけるデータセキュリティに関し、特に着脱可能な記録媒体（リムーバブルメディア）におけるデータの保護に関する。

【０００２】

【従来の技術】

コンピュータの外部記憶装置として、システムへの着脱が可能なリムーバブル

メディアを用いた装置がある。リムーバブルメディアは、記録媒体のみを記憶装置から取り出せることから可搬性に優れ、またコンピュータに装着して直ちに利用できる利便性を持つため、広く普及している。このリムーバブルメディアには、ＰＣＭＣＩＡ（Personal Computer Memory Card International Association）スロットで使われるＡＴＡ（AT Attachment）カードやＵＳＢポートに装着して用いられるＵＳＢカード、専用のディスクドライブ（駆動装置）に装着して使用される磁気ディスクや光ディスクなど、様々な種類のものが存在する。

【０００３】

この種のリムーバブルメディアは、上述したように記憶装置に対して着脱自在であり、かつ対応するポートや駆動装置を持つコンピュータであれば装着して利用可能であるため、格納されるデータの種類によっては、十分なデータ保護の対策が必要である。

従来、リムーバブルメディアにおけるデータ保護の手段としては、書き込み禁止や格納するデータファイルを隠しファイルとすることが一般的であるが、これらの手段を用いても、記録媒体に書き込まれたデータ自体はコンピュータが読み取り可能な形式であるため、秘匿性が低く、悪意を持ったユーザによるデータの読み取りが可能であった。

【０００４】

データ保護のための強力な手段として、記録媒体に格納するデータファイルを暗号化する方法がある（例えば、特許文献１参照）。これによれば、暗号化されたデータファイルを復号するための情報（復号キー）を持つユーザのみがデータを利用できることとなるため、十分なデータ保護を図ることができる。

データを暗号化する際の一般的な手順としては、まずＯＳ（オペレーティングシステム）や暗号化ツール（プログラム）の暗号化機能を呼び出して、各ツールのユーザインターフェイスに従って、パスフレーズの入力その他の操作を行っていた。

同様に、暗号化されたデータを復号する際にも、まずＯＳや暗号化ツールの復号化機能を呼び出して、各ツールのユーザインターフェイスに従って、パスフレーズの入力その他の操作を行っていた。

なお、特許文献１に開示された技術は、入力されるパスフレーズそのものを用いてデータの暗号化や復号化を行うのではなく、パスフレーズから生成されるキーデータを用い、復号の際にはこのキーデータを要求するなど、さらにセキュリティを高める工夫がなされているが、操作手順における本質的な差異はない。

【０００５】

【特許文献１】

特開平９－２３７２２８号公報（第３頁）

【０００６】

【発明が解決しようとする課題】

上述したように、リムーバブルメディアに格納されたデータを保護する手段としては、当該データファイルを暗号化することが極めて効果的である。しかし、上述したように、従来のＯＳや暗号化ツールの暗号化機能を利用してデータファイルの暗号化を行う場合、データファイルの暗号化および復号化を行う度にパスフレーズの入力その他の煩雑な操作を行う必要があり、ユーザにとって必ずしも使い勝手の良いものとは言えなかった。

【０００７】

特に、リムーバブルメディアの着脱に伴って、記録されているデータファイルの暗号化および復号化を行う場合、かかる処理を行うための操作を簡便にすることが望まれていた。

そこで本発明は、データファイルの暗号化および復号化における操作を簡単化し、リムーバブルメディアに適したデータ保護の手段を提供することを目的とする。

【０００８】

【課題を解決するための手段】

上記の目的を達成する本発明は、次のように構成された情報処理装置として実現される。すなわち、この情報処理装置は、コンピュータ本体と、このコンピュータ本体に設けられたコネクタを介して着脱自在に接続された外部記憶装置とを備える。そして、コンピュータ本体は、外部記憶装置に対するイジェクション要求を受け付ける受け付け手段と、この受け付け手段にてイジェクション要求が受

け付けられたことを条件に、外部記憶装置に格納されている所定のデータファイルを暗号化する暗号化手段とを備えることを特徴とする。

この情報処理装置は、暗号化の完了した外部記憶装置へのアクセスを停止して物理的に取り外すことを可能とするためのデバイス停止手段や、暗号化手段による暗号化に用いられるパスフレーズの入力を受け付けて管理するパスフレーズ管理手段をさらに備える構成とすることができる。

【０００９】

また、本発明による他の情報処理装置は、コンピュータ本体が、コネクタに外部記憶装置を接続したことによって発行される装着イベントを検出するイベント検出手段と、このイベント検出手段により装着が検出された外部記憶装置に暗号化されたデータファイルが格納されているか否かを調べる暗号化ファイル検出手段と、この暗号化ファイル検出手段にて検出された、暗号化されたデータファイルを、予め設定されたパスフレーズを用いて復号する復号化手段とを備えることを特徴とする。

【００１０】

さらにまた、上記の目的を達成する他の本発明は、コンピュータに接続された外部記憶装置に格納されているデータファイルに対して暗号処理を施す、次のように構成された暗号処理システムとしても実現される。この暗号処理システムは、イジェクション時にデバイスへのアクセス停止処理を含むソフトウェア制御を行う仕様でコンピュータに接続された外部記憶装置に対するイジェクション要求を受け付ける受け付け手段と、この受け付け手段にてイジェクション要求が受け付けられたことを条件に、外部記憶装置に格納されている所定のデータファイルを暗号化する暗号化手段とを備えることを特徴とする。

この暗号処理システムは、コンピュータに外部記憶装置が接続されたことを検知して、この外部記憶装置に格納されている暗号化されたデータファイルを復号化する復号化手段や、暗号化手段による暗号化および復号化手段による復号化に用いられるパスフレーズを管理するパスフレーズ管理手段をさらに備える構成とすることができる。

【００１１】

また、上記の目的を達成するさらに他の本発明は、コンピュータに接続された外部記憶装置の制御方法としても実現される。この外部記憶装置の制御方法は、ユーザによる操作を受け付けて、イジェクション時にデバイスへのアクセス停止処理を含むソフトウェア制御を行う仕様でコンピュータに接続された外部記憶装置に対するイジェクション要求を発行するステップと、このイジェクション要求が発行されたことを条件に、外部記憶装置に格納されている所定のデータファイルを読み出して暗号化し、再び外部記憶装置に格納するステップとを含むことを特徴とする。

【００１２】

さらに、本発明による他の外部記憶装置の制御方法は、コンピュータに外部記憶装置が接続されたことを検知して、この外部記憶装置に暗号化されたデータファイルが格納されているか否かを調べるステップと、この外部記憶装置に暗号化されたデータファイルが格納されている場合に、この暗号化されたデータファイルを読み出し、予め設定され所定の記憶手段にて保持されているパスフレーズを用いてこの暗号化されたデータファイルを復号し、再び外部記憶装置に格納するステップとを含むことを特徴とする。

【００１３】

さらに本発明は、コンピュータを制御して上述した暗号処理システムの各機能を実現させるプログラム、またはコンピュータに上記の外部記憶装置の制御方法における各ステップに相当する処理を実行させるプログラムとしても実現される。このプログラムは、磁気ディスクや光ディスク、半導体メモリ、その他の記録媒体に格納して配布したり、ネットワークを介して配信したりすることにより、提供することができる。

【００１４】

【発明の実施の形態】

以下、添付図面に示す実施の形態に基づいて、この発明を詳細に説明する。

図１は、本発明の実施の形態によるデータ保護方式を実現するのに好適なコンピュータ装置のハードウェア構成の例を模式的に示す図である。

図１に示すように、本実施の形態に用いられるコンピュータ装置は、各種の処

理および制御を行うＣＰＵ１１と、ＣＰＵ１１の動作を制御するプログラムやＣＰＵ１１の処理において使用されるメモリ１２と、外部記憶装置を制御するためのＰＣＭＣＩＡコントローラ１３およびＵＳＢコントローラ１４と、ユーザインターフェイス画面を表示するためのビデオコントローラ１５および表示装置１６とを備える。ＰＣＭＣＩＡコントローラ１３にはＰＣカードを装着するスロット（ＰＣＭＣＩＡコネクタ）が設けられており、このスロットに外部記憶装置としてリムーバブルメディアであるＡＴＡカードを装着することができる。またＵＳＢコントローラ１４にはＵＳＢコネクタが設けられており、このＵＳＢコネクタに外部記憶装置としてリムーバブルメディアであるＵＳＢメモリを装着することができる。

【００１５】

なお、図１は本実施の形態を実現するコンピュータ装置のハードウェア構成を例示するに過ぎず、本実施の形態を適用可能であれば、他の種々の構成を取ることができる。例えば、外部記憶装置としては、上述したＰＣＭＣＩＡコントローラ１３やＵＳＢコントローラ１４を介して接続される装置の他、一般に、ＩＤＥ（Integrated Device Electronics）やＳＣＳＩ（Small Computer System Interface）インターフェイスを介して接続されたハードディスクが接続される。さらに、特に図示しないが、キーボードやマウス等の入力デバイスがそれぞれのインターフェイスを介して接続される。

【００１６】

本実施の形態では、リムーバブルメディアとして、ＡＴＡカードとＵＳＢメモリとを想定して、以下の説明を行う。ＰＣＭＣＩＡやＵＳＢでは、データ保護の観点からソフトウェア制御を含むイジェクションが行われる。すなわち、ＡＴＡカードやＵＳＢメモリ（以下、これらを特に区別しない場合は、単に記録媒体と称す）を取り外す際には、まずソフトウェアレベルでイジェクションのための処理が行われ、メモリ１２に一時的に保持されているデータが記録媒体に格納される（フラッシュ）と共にデバイスのアクセス停止処理が行われる。この後にＡＴＡカードやＵＳＢメモリを物理的にスロットやコネクタから取り外すことが許される。したがって、本実施の形態では、このソフトウェア制御の時点で、データ

ファイルの暗号化を実行する。

なお、磁気ディスクや光ディスクの駆動装置では、これらのディスク状記録媒体を駆動装置から抜き取る際に、上記のようなソフトウェア制御を行うことは通常想定されていない。しかし、データ保護の観点からは、これらの装置においてもデータ保護の観点からは上記のようにメモリ１２の内容をフラッシュしてからディスクを取り出すようにすることが好ましい。そして、そのようなソフトウェア制御を行っているシステムにおいては、磁気ディスクや光ディスクに対しても本実施の形態による暗号化および復号化の処理（以下、これらの処理を特に区別しない場合、暗号処理と総称する）をそのまま適用することが可能である。

さらにまた、ＰＣＭＣＩＡやＵＳＢのコネクタにてコンピュータ装置に接続されるディスク状記録媒体の駆動装置を当該コネクタ部分で取り外す場合は、上述したＡＴＡカードやＵＳＢメモリと同様のソフトウェア制御が行われるので、本実施の形態による暗号処理をそのまま適用することができる。

【００１７】

図２は、コンピュータにおいて本実施の形態によるデータ保護方式を実現する暗号処理システムの機能構成を示す図である。

図２を参照すると、本実施の形態の暗号処理システム１００は、記録媒体の着脱に応じて処理を実行するためのデバイス装着イベント検出部１１０およびデバイスイジェクション処理部１２０と、データファイルに対する暗号処理およびその制御を行うための暗号処理起動部１３０、ファイル管理部１４０および暗号処理部１５０と、ユーザに情報を提供すると共にユーザからの指示を受け付けるユーザインターフェイス処理部１６０とを備える。

これらの各構成要素は、例えば図１に示したコンピュータ装置にて実現する場合、メモリ１２に格納されているプログラムにて制御されたＣＰＵ１１の機能として実現される。ＣＰＵ１１を制御するプログラムは、磁気ディスクや光ディスク、半導体メモリ、その他の記録媒体に格納して配布したり、ネットワークを介して配信したりすることにより、提供することができる。

【００１８】

また、図２に示すように、暗号処理システム１００は、ＯＳ（オペレーティン

グシステム）２００上で動作するアプリケーションにて実現されている。ＯＳ２００は、図１に示したＰＣＭＣＩＡコントローラ１３を制御するＰＣＭＣＩＡデバイスドライバ２１１、ＵＳＢコントローラ１４を制御するＵＳＢデバイスドライバ２１２を備える。そして、これらのデバイスドライバの動作から得られるイベントを暗号処理システム１００へ送ると共に、暗号処理システム１００からの指示に従って記録媒体のイジェクションに伴うデバイス停止処理を各デバイスドライバに実行させる（デバイス停止手段としての機能）。

【００１９】

図２に示した暗号処理システム１００の構成において、デバイス装着イベント検出部１１０は、ＯＳ２００から送られるイベント通知から記録媒体の装着イベント（記録媒体がコントローラに装着されたことを通知するイベント）が検出されたならば、その記録媒体に格納されたデータファイル（またはその一部）に対して復号化処理が必要かどうかを判断する。そして、復号化処理の必要な（すなわち暗号化された）データが含まれている場合は、暗号処理起動部１３０に復号化処理要求を送る。暗号化されたデータの有無は、データファイルの識別子等の付加情報から判断することができる。

【００２０】

デバイスイジェクション処理部１２０は、後述する記録媒体のイジェクション時の暗号処理が終了した後に、記録媒体へのアクセスを停止させる要求をＯＳ２００に通知する。これにより、必要に応じてメモリ１２の記憶内容がフラッシュされ、デバイスドライバから記録媒体へのアクセスが停止されて、記録媒体をコントローラから取り外す（物理的に切断する）準備が完了する。

【００２１】

暗号処理起動部１３０は、デバイス装着イベント検出部１１０から復号化処理要求を受け取った場合に復号化処理を開始し、また記録媒体を取り外す際のソフトウェア制御として暗号化処理を開始するため、暗号化・復号化ファイル管理部に対して動作指示を行う。

【００２２】

ファイル管理部１４０は、記録媒体のファイル構造を管理し、フォルダ単位ま

たはファイル単位でデータの読み出し及び書き込み制御を行う。また、記録媒体から読み出されて復号化されたデータをＯＳ２００のファイル・システム上で正しく処理できるように、ファイルの属性や日付などのファイル情報をファイルヘッダに記述する後処理を行う。さらに、記録媒体のイジェクションに際し、暗号化されたデータファイルに対して識別子を作成し、ファイルヘッダにファイル情報を記述する等の後処理を行う。

【００２３】

暗号処理部１５０は、データファイルの暗号化および復号化の処理を実行する。暗号化や復号化に用いられるアルゴリズムとしては、ＲＣ４、ＲＣ５、ＡＥＳなどの標準アルゴリズムを利用することができる。なお、暗号処理部１５０は、上述したようにプログラム制御されたＣＰＵ１１にてソフトウェア的に実現する他、暗号回路を内蔵した専用のチップ（ハードウェア）にて実現しても良い。暗号処理の具体的な動作については後述する。

【００２４】

ユーザインターフェイス処理部１６０は、ユーザによる暗号処理のための操作を受け付け、ユーザに各種の情報を提供する。具体的には、記録媒体をコントローラから取り外す際の動作として、イジェクション要求を受け付けて、暗号処理起動部１３０を起動させる（イジェクション要求の受け付け手段としての機能）。このイジェクション要求は、例えば図１に示した表示装置１６に表示されたアイコンを操作して発行しても良いし、キーボードに予め設定された特定のホットキーを操作して発行しても良い。イジェクションにおけるソフトウェア制御においてＯＳ２００による記録媒体へのアクセスの停止処理が正常完了したならば、ユーザインターフェイス処理部１６０は、ビデオコントローラ１５を介して、コントローラから記録媒体を物理的に取り外すことを許す旨のメッセージを表示装置１６に表示する。

また、ユーザインターフェイス処理部１６０は、ビデオコントローラ１５を介して表示装置１６に後述するユーザインターフェイス画面を表示する。そして、ユーザによるこのユーザインターフェイス画面への操作によって、暗号化および復号化に用いられるパスフレーズの入力や、暗号化対象のファイルまたはフォル

ダの指定といったオプション設定を行うことができる。この設定情報は、メモリ１２やハードディスクに保持され、ユーザインターフェイス処理部１６０にて管理される（パスフレーズを含む設定情報の管理手段としての機能）。

【００２５】

図３および図４は、ユーザインターフェイス画面の例を示す図である。

図３に示すユーザインターフェイス画面では、処理対象の記録媒体（Device）、暗号処理を行うか否か（Action）、暗号化対象フォルダ（Encrypted Folders）の各項目を選択することができる。図示の例では、記録媒体「IBM Microdrive 340MB」におけるフォルダ「Planning」に対して暗号化を行う（Enable data encryption）ように設定されている。図３のユーザインターフェイス画面の下部にあるボタン「Encryption settings...」をクリックすると、図４のユーザインターフェイス画面に移行する。

図４のユーザインターフェイス画面では、フォルダ「Planning」の下位におけるどのファイルまたはフォルダを暗号処理するかについてさらに細かく指定できる。また、入力フィールド４０１にパスフレーズを入力する。

図３、図４のユーザインターフェイス画面で暗号処理の設定を行い、ＯＫボタンをクリックすることにより、かかる設定が有効となる。図示の例では、記録媒体「IBM Microdrive 340MB」のイジェクションの際、この記録媒体に格納されているフォルダ「Planning」内のデータファイルが暗号化されることとなる。

【００２６】

次に、上記のように構成された暗号処理システムによる暗号処理の動作について説明する。

図５は、本実施の形態による記録媒体のイジェクション時の動作を説明するフローチャートである。

図５に示すように、ユーザによる記録媒体のイジェクション要求が発行されると（ステップ５０１）、ユーザインターフェイス処理部１６０は、この要求を受け付け、暗号処理の設定情報を参照して、この要求が管理下にある記録媒体（すなわちＰＣＭＣＩＡやＵＳＢのリムーバブルメディア）かどうかを調べる（ステップ５０２）。管理下にある記録媒体でなければ、デバイスイジェクション処理

部１２０を介して、この要求を直ちにＯＳ２００へ送信して処理を終了する（ステップ５０７）。

【００２７】

イジェクション要求にかかる記録媒体がユーザインターフェイス処理部１６０の管理下にある記録媒体である場合は、次に、この記録媒体に格納されているフォルダあるいはファイルのうち、暗号化対象として指定されているものがあるかどうかを調べる（ステップ５０３）。この指定がない場合は、暗号処理を行う必要がないので、デバイスイジェクション処理部１２０を介して、イジェクション要求をＯＳ２００へ送信して処理を終了する（ステップ５０７）。

【００２８】

暗号化対象の指定がある場合は、暗号処理起動部１３０に処理が移行してファイル管理部１４０が起動し、暗号化対象のフォルダまたはファイルを記録媒体から読み出して暗号処理部１５０にて暗号化する（ステップ５０４）。これに伴って、ファイル管理部１４０により、ファイルヘッダへの記述等の後処理が行われる。これらの処理によって、記録媒体における暗号化対象であった元データが暗号化されたデータに書き換えられる。暗号化の処理が正常終了したならば、デバイスイジェクション処理部１２０を介して、イジェクション要求をＯＳ２００へ送信して処理を終了する（ステップ５０５、５０７）。

一方、暗号化の処理が正常に終了しなかった場合は、ユーザインターフェイス処理部１６０によって表示装置１６にエラー表示が行われる（ステップ５０５、５０６）。そして、デバイスイジェクション処理部１２０を介して、イジェクション要求をＯＳ２００へ送信して処理を終了する（ステップ５０７）。この場合、格納されているデータファイルは暗号化されずに記録媒体のイジェクションが行われることとなる。

【００２９】

図６は、本実施の形態による記録媒体の装着時の動作を説明するフローチャートである。

図６に示すように、ＰＣＭＣＩＡコントローラ１３やＵＳＢコントローラ１４に記録媒体が装着されると、デバイス装着イベント検出部１１０にて記録媒体の

装着イベントが検出され（ステップ６０１）、装着された記録媒体のタイプがチェックされる（ステップ６０２）。装着された記録媒体がＰＣカード（ＡＴＡカード）やＵＳＢメモリでなければ、何も行わずに処理を終了する。

一方、装着された記録媒体がＰＣカードやＵＳＢメモリである場合は、次に、この記録媒体に格納されているデータのうち、復号対象、すなわち暗号化されたものがあるかどうかを調べる（ステップ６０３）。復号対象がない場合は、復号化処理を行う必要がないので、何も行わずに処理を終了する。

【００３０】

記録媒体に格納されているデータに復号対象がある場合は、デバイス装着イベント検出部１１０から暗号処理起動部１３０へ復号化処理要求が送られ、ファイル管理部１４０が起動し、復号対象のデータを記録媒体から読み出して暗号処理部１５０にて復号する（ステップ６０４）。これに伴って、ファイル管理部１４０により、ファイルヘッダへの記述等の後処理が行われる。これらの処理により、記録媒体における復号化対象であったデータが復号化されたデータに書き換えられる。復号化の処理が正常に終了したならば、これ以降ＯＳ２００から復号されたデータへのアクセスが可能となり、処理が終了する（ステップ６０５）。

一方、暗号化の処理が正常に終了しなかった場合は、ユーザインターフェイス処理部１６０によって表示装置１６にエラー表示が行われた後、処理が終了する（ステップ６０５、６０６）。この場合、記録媒体に格納されている暗号化されたデータは復号化されておらず、ＯＳ２００からアクセスして利用することはできない。

【００３１】

本実施の形態では、上述したようにパスフレーズを含む設定情報はユーザインターフェイス処理部１６０に管理されてコンピュータ装置に保持されているので、暗号処理のたびにパスフレーズを入力する必要はない（ただし、オプションで毎回パスフレーズを入力する設定とすることはできる）。しかし、他のコンピュータ装置で暗号化された記録媒体を装着した場合、当該記録媒体に格納されている暗号化されたデータが、当該コンピュータ装置に保持されているパスフレーズで復号できるとは限らない。そこで、暗号処理部１５０は、記録媒体に暗号化さ

れたデータが格納されており、かつユーザインターフェイス処理部１６０にて管理されているパスワードでは当該データを復号できない場合に、例えばパスフレーズ入力用のダイアログメッセージを表示装置１６に表示させ、ユーザにパスフレーズの入力を促すことができる。

【００３２】

図７は、本実施の形態による暗号処理部１５０の暗号化処理の動作を説明する図である。

図７を参照すると、暗号処理部１５０は、データ処理手段として、暗号化対象であるデータを暗号化する暗号化エンジン１５１と、当該データのハッシュ値を生成するハッシュ値生成エンジン１５２と、パスフレーズを喪失した際に用いるヒント情報を暗号化するヒント情報暗号化エンジン１５３とを備える。なお、暗号化エンジン１５１とヒント情報暗号化エンジン１５３とは、実際には同一のエンジンを用いても良い。

【００３３】

図７に示すように、暗号化エンジン１５１は、パスフレーズと暗号化対象のデータとを入力し、当該パスフレーズに基づいて当該データを暗号化して出力する（以下、暗号化エンジン１５１にて暗号化されたデータを暗号化データ、暗号化データに所定のヘッダ情報が付加されたものを暗号化ファイルと称す）。暗号化のアルゴリズムは、ＲＣ２、ＲＣ４、ＲＣ６、３ＤＥＳ、ＡＥＳなど、種々のものを用いることができ、かつ動的に変更して適用することができる。暗号化のアルゴリズムを動的に変更することにより、セキュリティをさらに高めることができる。

ハッシュ値生成エンジン１５２は、パスフレーズと暗号化対象のデータとを入力し、当該パスフレーズに基づいて当該データのハッシュ値を計算して出力する。ハッシュ値を計算するハッシュ関数としては、例えばＭＤ５を用いることができる。

ヒント情報暗号化エンジン１５３は、暗号化対象のデータの属性や作成された日付等のファイル情報と所定のヒントストリングとを入力し、暗号化して出力する。ヒントストリングは、ユーザがパスフレーズを喪失した際に、パスフレーズ

を得るためのヒントとなる情報を含むデータ（文字列）である。なお、ヒントストリングを暗号化して暗号化ファイルに付加することは必須の要件ではない。

【００３４】

図７に示すように、暗号処理部１５０の処理により生成される暗号化ファイルには、暗号化エンジン１５１から出力された暗号化データの他、ヘッダ情報として、暗号化対象であった元データのファイル情報と、ハッシュ値生成エンジン１５２から出力されたデータ（元データ）のハッシュ値と、ヒント情報暗号化エンジン１５３から出力されたヒント情報の暗号化データとが記述される。

【００３５】

図８は、本実施の形態による暗号処理部１５０の復号化処理の動作を説明する図である。

図８を参照すると、暗号処理部１５０は、データ処理手段として、暗号化データを復号する復号化エンジン１５４と、パスフレーズの正当性を検証するパスフレーズ検証手段１５５と、暗号化されたヒント情報を復号するヒント情報復号化エンジン１５６とを備える。なお、復号化エンジン１５４とヒント情報復号化エンジン１５６とは、実際には同一のエンジンを用いても良い。

【００３６】

図８に示すように、復号化エンジン１５４は、パスフレーズと暗号化ファイル中の暗号化データとを入力し、復号して出力する。暗号化エンジン１５１に対応して、復号化のアルゴリズムは種々のものを用いることができ、かつ動的に変更して適用することができる。

パスフレーズ検証手段１５５は、復号化エンジン１５４にて復号化されたデータ（以下、復号データ）からパスフレーズに基づいて計算されるハッシュ値と、暗号化ファイルのファイルヘッダに記述されている元データのハッシュ値とを入力して比較し、その正当性を検証する。パスフレーズを用いて復号データからハッシュ値を計算するには、暗号化の際に用いられたハッシュ値生成エンジン１５２を使う。すなわち、パスフレーズおよび復号データのハッシュ値を求める計算は、暗号化の場合におけるパスフレーズおよび元データのハッシュ値を求める計算と同一である。したがって、暗号化ファイルが改竄されていなければ、元デー

タと復号データとは同一であるため、ハッシュ値も同一であることが期待される。このようにして、ハッシュ値の比較結果により暗号化ファイルの正当性を検証することができる。

ヒント情報復号化エンジン１５６は、暗号化ファイルのファイルヘッダに記述されている元ファイル（暗号化前のファイル）のファイル情報と、ヒント情報の暗号化データとを入力し、復号化する。復号化されたヒントストリングは、例えば表示装置１６に表示出力される。これによりユーザは、パスフレーズを知る手掛かりとなるヒント情報が得られる。

【００３７】

【発明の効果】

以上説明したように、本発明によれば、データファイルの暗号化および復号化における操作を簡単化し、リムーバブルメディアに適したデータ保護の手段を提供することができる。

【図面の簡単な説明】

【図１】　本発明の実施の形態によるデータ保護方式を実現するのに好適なコンピュータ装置のハードウェア構成の例を模式的に示す図である。

【図２】　コンピュータにおいて本実施の形態によるデータ保護方式を実現する暗号処理システムの機能構成を示す図である。

【図３】　本実施の形態にて用いられるユーザインターフェイス画面の例を示す図である。

【図４】　本実施の形態にて用いられるユーザインターフェイス画面の他の例を示す図である。

【図５】　本実施の形態による記録媒体のイジェクション時の動作を説明するフローチャートである。

【図６】　本実施の形態による記録媒体の装着時の動作を説明するフローチャートである。

【図７】　本実施の形態による暗号処理部の暗号化処理の動作を説明する図である。

【図８】　本実施の形態による暗号処理部の復号化処理の動作を説明する図

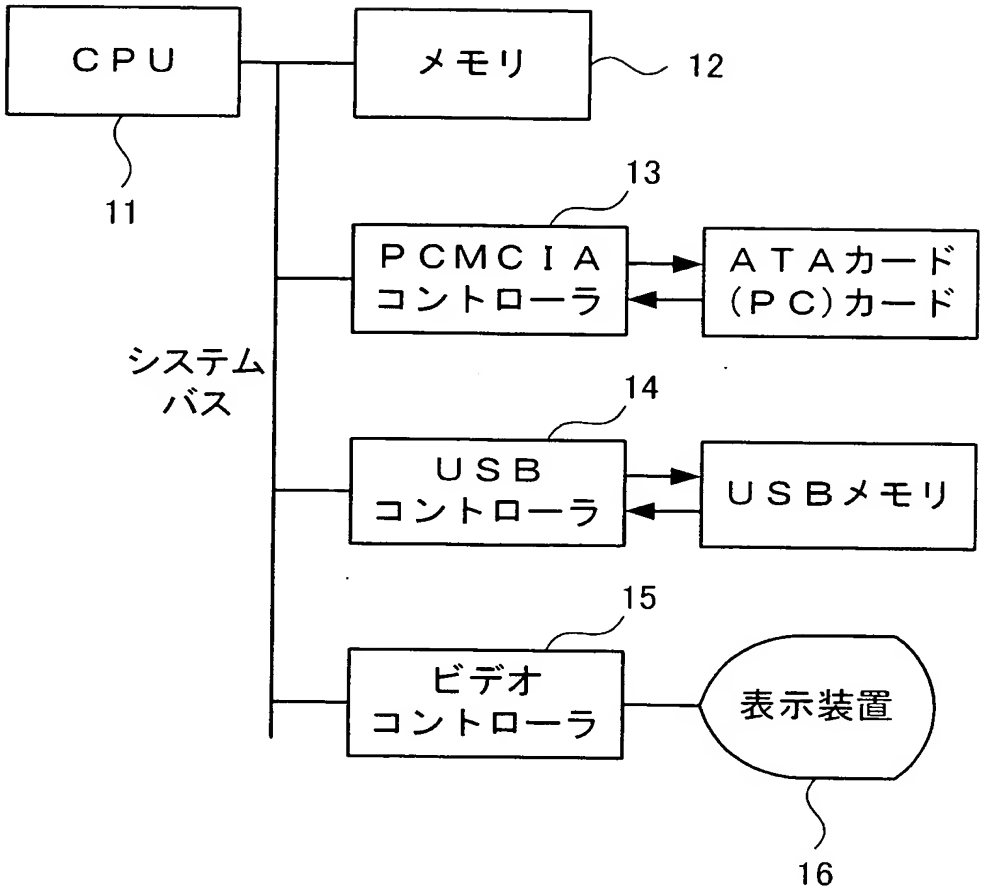
である。

【符号の説明】

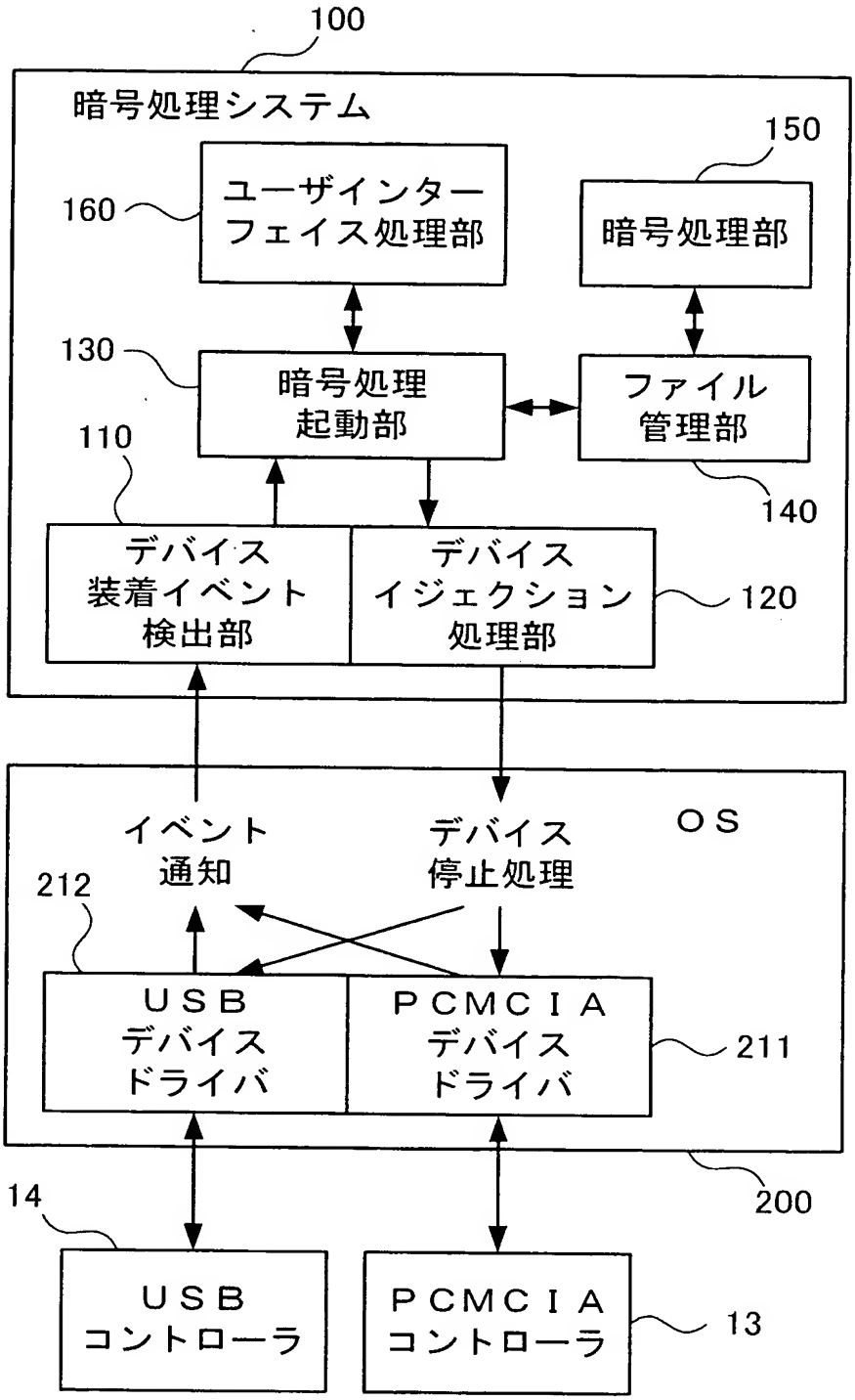
１１…ＣＰＵ、１２…メモリ、１３…ＰＣＭＣＩＡコントローラ、１４…ＵＳＢコントローラ、１５…ビデオコントローラ、１６…表示装置、１００…暗号処理システム、１１０…デバイス装着イベント検出部、１２０…デバイスイジェクション処理部、１３０…暗号処理起動部、１４０…ファイル管理部、１５０…暗号処理部、１５１…暗号化エンジン、１５２…ハッシュ値生成エンジン、１５３…ヒント情報暗号化エンジン、１５４…復号化エンジン、１５５…パスフレーズ検証手段、１５６…ヒント情報復号化エンジン、１６０…ユーザインターフェイス処理部、２００…ＯＳ（オペレーティングシステム）、２１１…ＰＣＭＣＩＡデバイスドライバ、２１２…ＵＳＢデバイスドライバ

【書類名】　図面

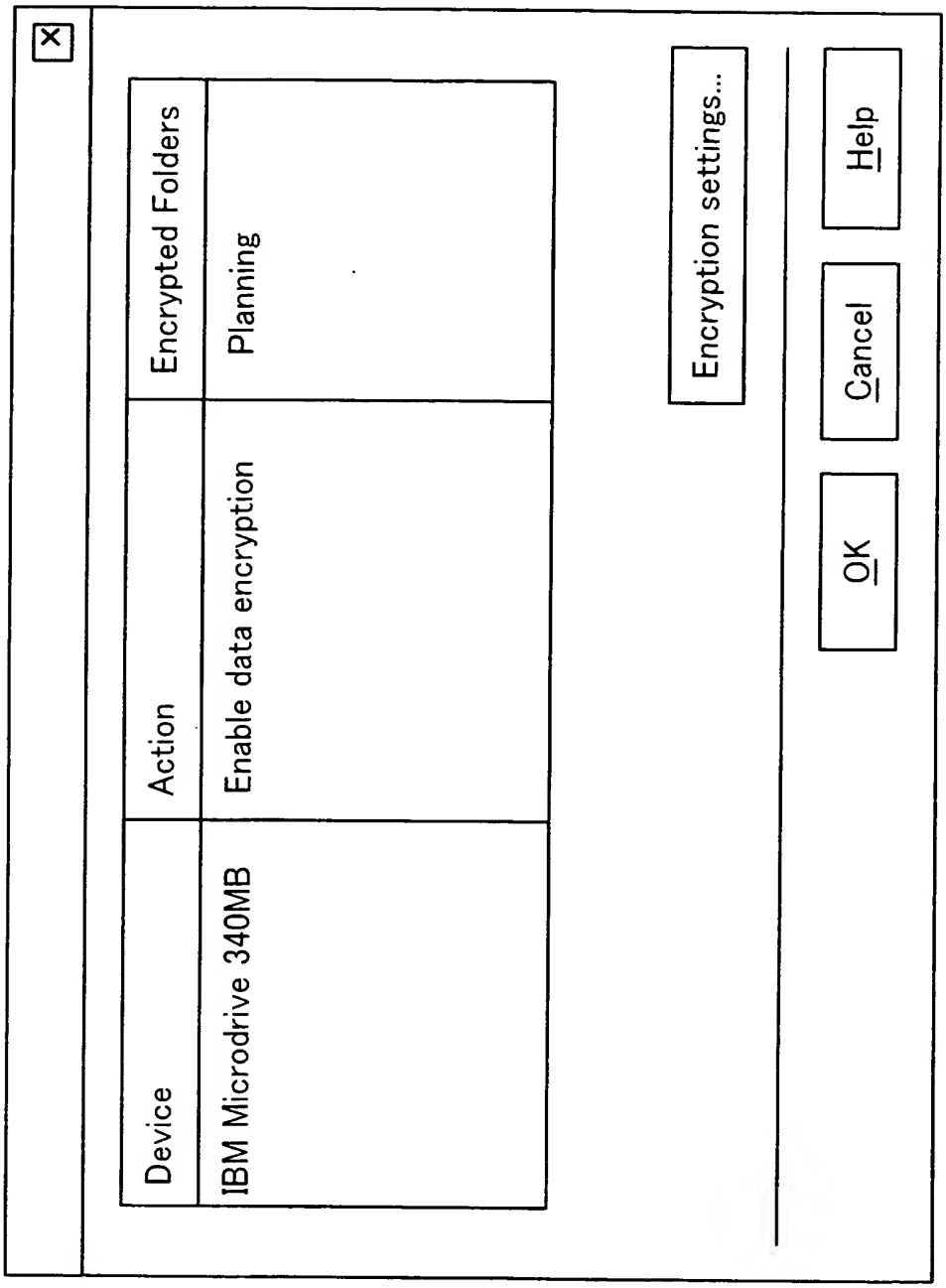
【図１】


ＣＰＵ
メモリ
12
11
13
ＰＣＭＣＩＡ
コントローラ
ＡＴＡカード
（ＰＣ）カード
システム
バス
14
ＵＳＢ
コントローラ
ＵＳＢメモリ
15
ビデオ
コントローラ
表示装置
16

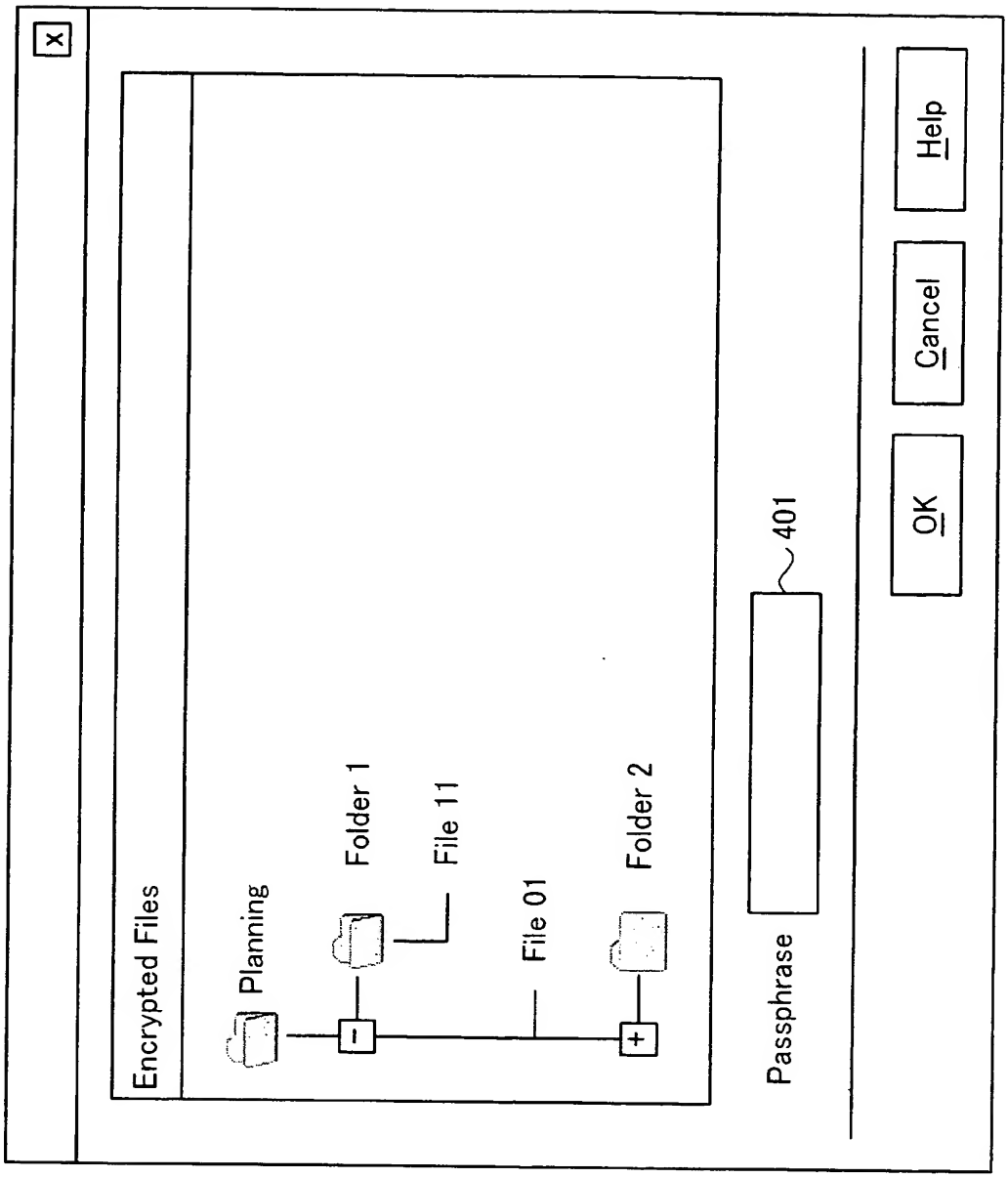
【図２】


100
暗号処理システム
150
160
ユーザインター
フェイス処理部
暗号処理部
130
暗号処理
起動部
ファイル
管理部
110
140
デバイス
装着イベント
検出部
デバイス
イジェクション
処理部
120
イベント
通知
デバイス
停止処理
ＯＳ
212
ＵＳＢ
デバイス
ドライバ
ＰＣＭＣＩＡ
デバイス
ドライバ
211
200
14
ＵＳＢ
コントローラ
ＰＣＭＣＩＡ
コントローラ
13

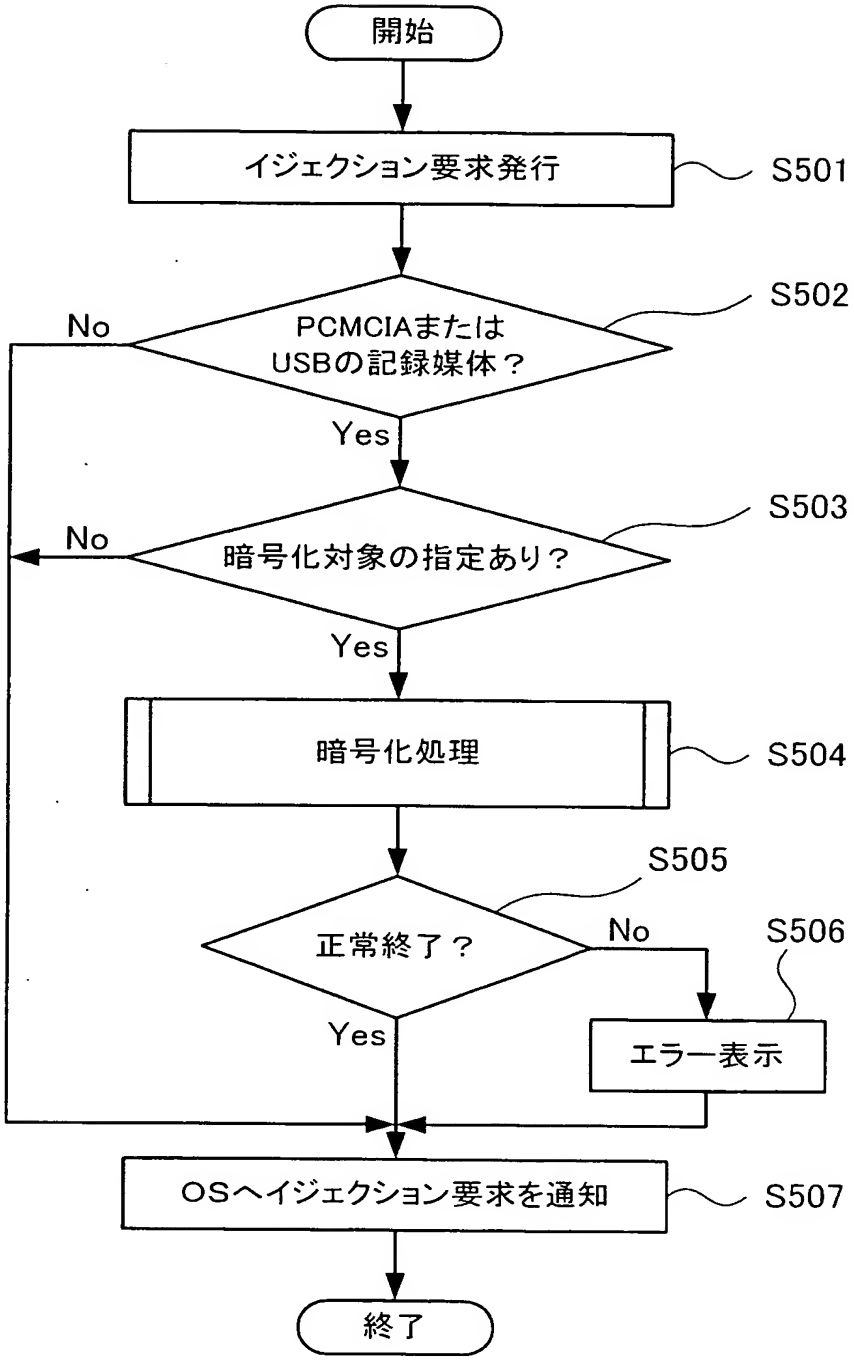
【図３】


Device
Action
Encrypted Folders
IBM Microdrive 340MB
Enable data encryption
Planning
Encryption settings...
OK
Cancel
Help

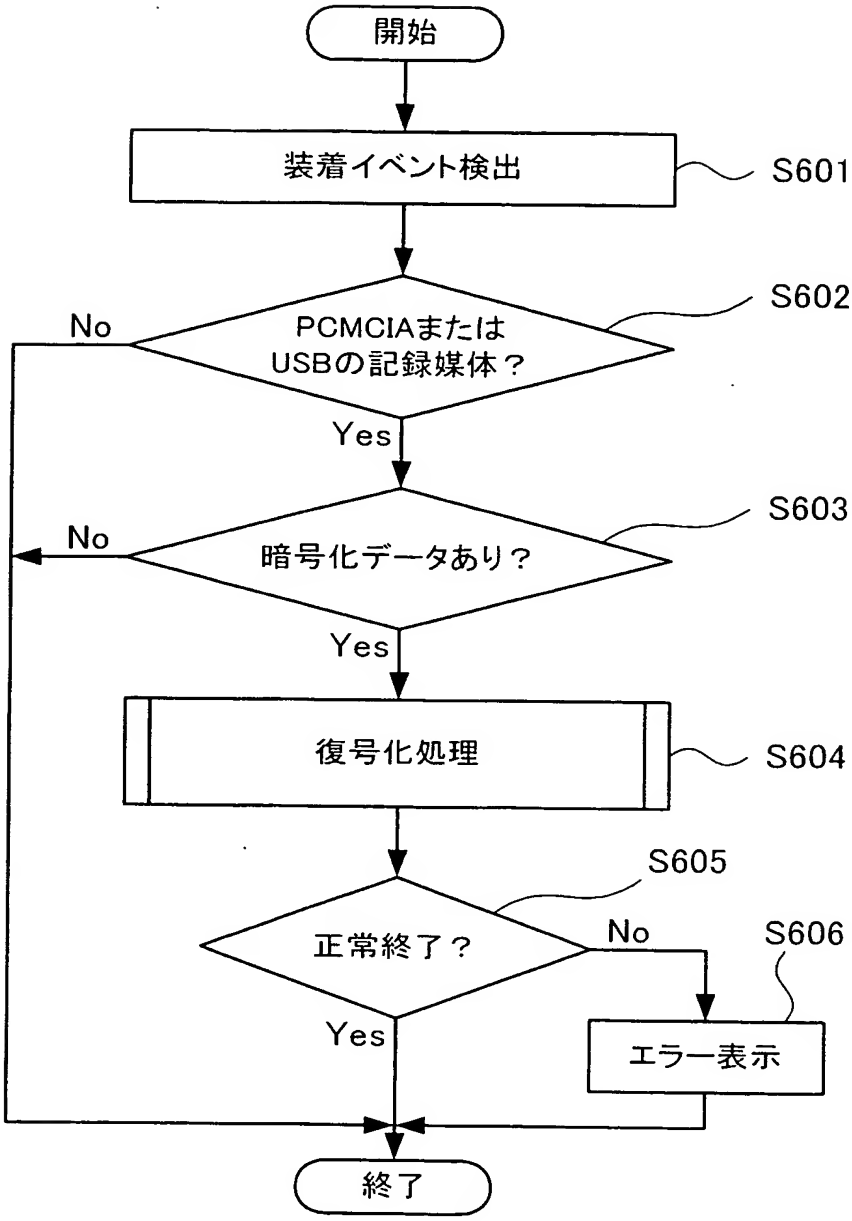
【図４】


Encrypted Files
Planning
Folder 1
File 11
File 01
Folder 2
401
Passphrase
OK
Cancel
Help

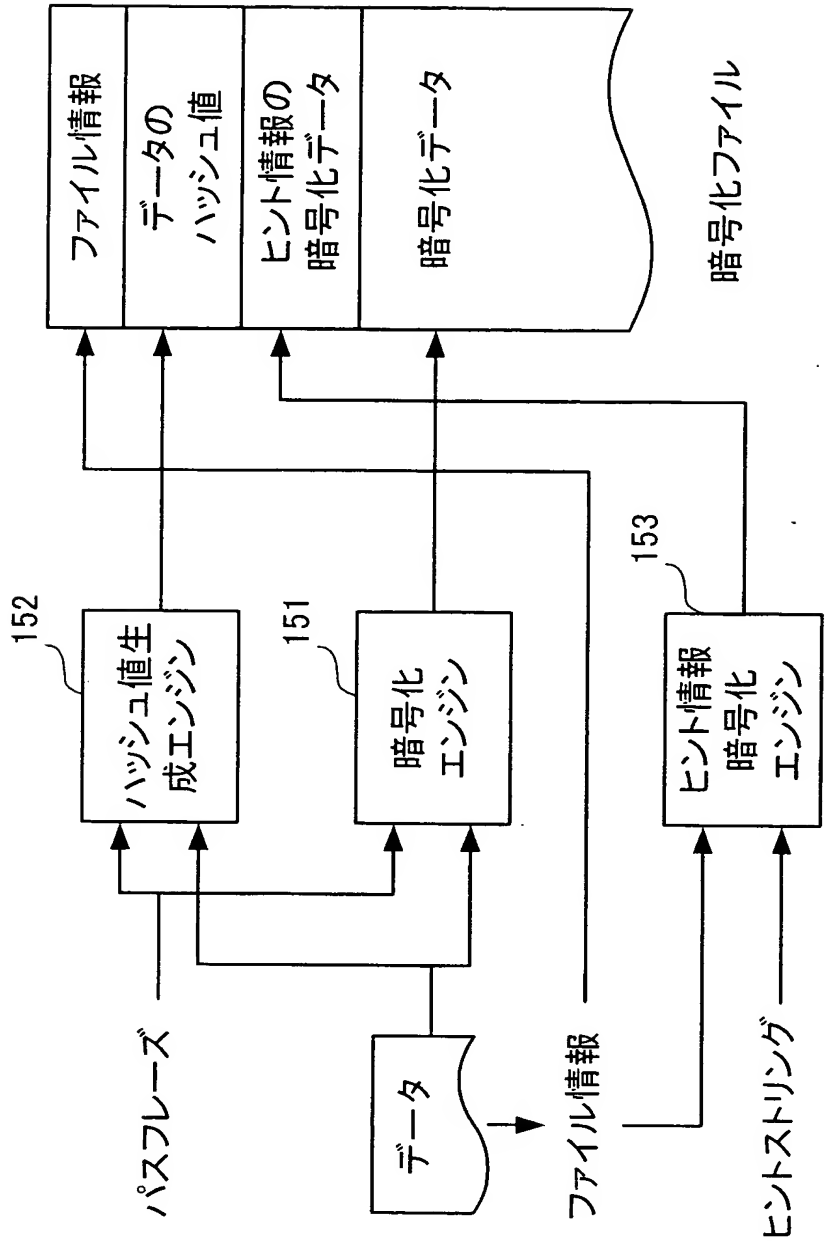
【図５】


開始
イジェクション要求発行
S501
PCMCIAまたは
USBの記録媒体？
S502
No
Yes
暗号化対象の指定あり？
S503
No
Yes
暗号化処理
S504
正常終了？
S505
No
S506
Yes
エラー表示
OSへイジェクション要求を通知
S507
終了

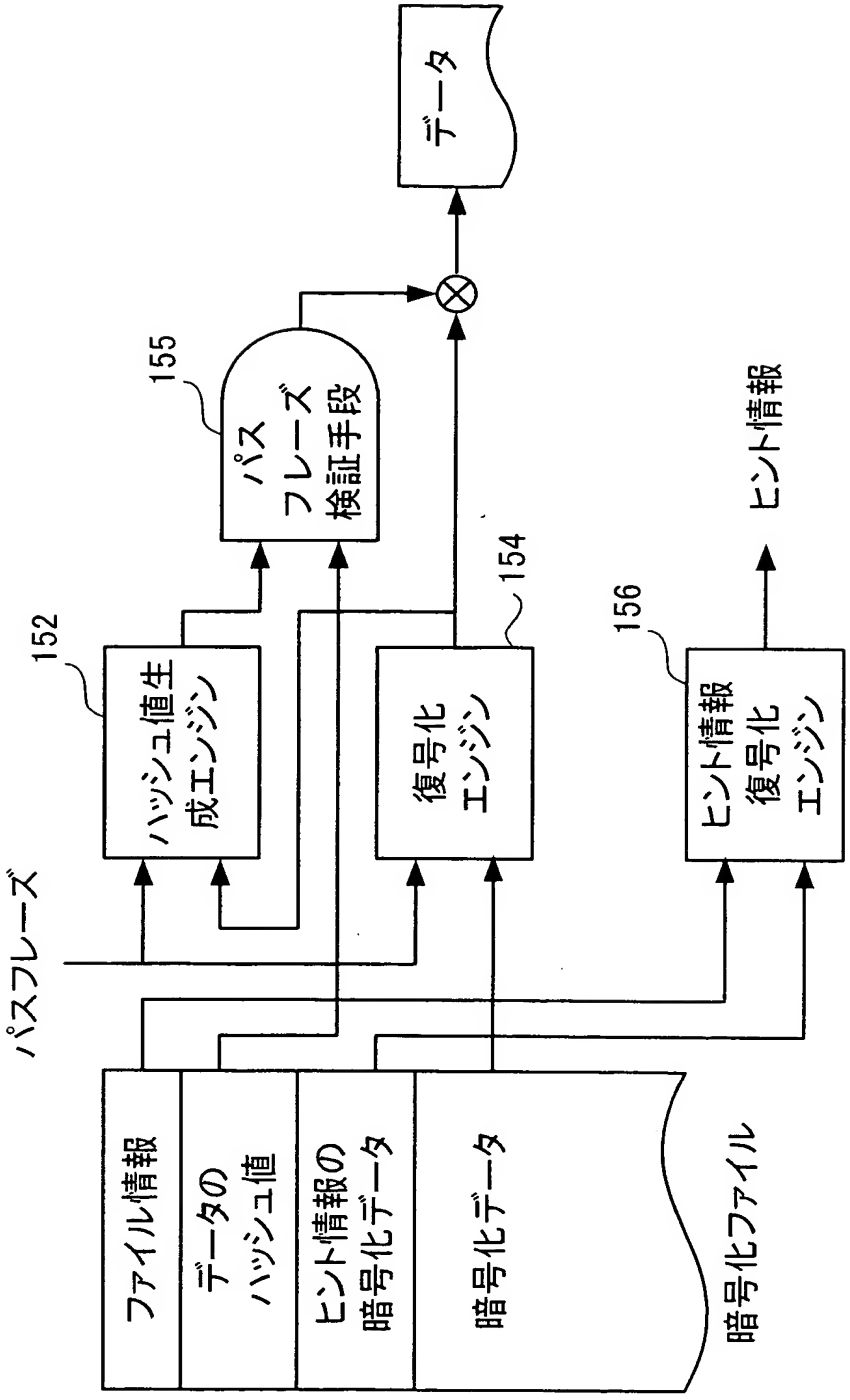
【図６】


開始
装着イベント検出
S601
PCMCIAまたは
USBの記録媒体？
S602
No
Yes
暗号化データあり？
S603
No
Yes
復号化処理
S604
正常終了？
S605
No
S606
Yes
エラー表示
終了

【図７】


ファイル情報
データのハッシュ値
ヒント情報の暗号化データ
暗号化データ
暗号化ファイル
152
ハッシュ値生成エンジン
151
暗号化エンジン
153
ヒント情報暗号化エンジン
パスフレーズ
データ
ファイル情報
ヒントストリング

【図８】


データ
155
パス
フレーズ
検証手段
ヒント情報
154
152
156
ハッシュ値生
成エンジン
復号化
エンジン
ヒント情報
復号化
エンジン
パスフレーズ
ファイル情報
データの
ハッシュ値
ヒント情報の
暗号化データ
暗号化データ
暗号化ファイル

【書類名】　　要約書

【要約】

【課題】　データファイルの暗号化および復号化における操作を簡単化し、リムーバブルメディアに適したデータ保護の手段を提供する。

【解決手段】　ＰＣＭＣＩＡやＵＳＢにてコンピュータに接続された外部記憶装置（記録媒体）に対するイジェクション要求を受け付けるユーザインターフェイス処理部１６０と、このユーザインターフェイス処理部１６０にてイジェクション要求が受け付けられたことを条件に、外部記憶装置に格納されている所定のデータファイルを暗号化する暗号処理起動部１３０、ファイル管理部１４０および暗号処理部１５０とを備える。また、コンピュータに外部記憶装置が接続されたことを検知するデバイス装着イベント検出部１１０を備え、暗号化する暗号処理起動部１３０、ファイル管理部１４０および暗号処理部１５０により、この外部記憶装置に格納されている暗号化されたデータファイルを復号化する。

【選択図】　　図２

認定・付加情報

特許出願の番号	特願２００３－０８５３５９
受付番号	５０３００４９２７５６
書類名	特許願
担当官	末武　実　　１９１２
作成日	平成１５年　５月　６日

＜認定情報・付加情報＞

【特許出願人】
- 【識別番号】 390009531
- 【住所又は居所】 アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
- 【氏名又は名称】 インターナショナル・ビジネス・マシーンズ・コーポレーション

【代理人】
- 【識別番号】 100086243
- 【住所又は居所】 神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内
- 【氏名又は名称】 坂口　博

【代理人】
- 【識別番号】 100091568
- 【住所又は居所】 神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内
- 【氏名又は名称】 市位　嘉宏

【代理人】
- 【識別番号】 100108501
- 【住所又は居所】 神奈川県大和市下鶴間１６２３番１４　日本アイ・ビー・エム株式会社　知的所有権
- 【氏名又は名称】 上野　剛史

【復代理人】 申請人
- 【識別番号】 100104880
- 【住所又は居所】 東京都港区赤坂５－４－１１　山口建設第２ビル６Ｆ　セリオ国際特許事務所
- 【氏名又は名称】 古部　次郎

【選任した復代理人】
- 【識別番号】 100118201

次頁有

認定・付加情報（続き）

【住所又は居所】　東京都港区赤坂５－４－１１　山口建設第二ビル
６Ｆ　セリオ国際特許事務所
【氏名又は名称】　千田　武

次頁無

特願２００３－０８５３５９

出　願　人　履　歴　情　報

識別番号　　［３９０００９５３１］

１．変更年月日　　２０００年　５月１６日
［変更理由］　名称変更
住　所　　アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　（番地なし）
氏　名　　インターナショナル・ビジネス・マシーンズ・コーポレーション

２．変更年月日　　２００２年　６月　３日
［変更理由］　住所変更
住　所　　アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
氏　名　　インターナショナル・ビジネス・マシーンズ・コーポレーション